International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 7, Issue.2, March-April 2024, page no. 273-278

To cite this article: Ifeoluwa Elegbe (2024). CYBER HYGIENE: ENHANCING CYBER HYGIENE PRACTICES TO MITIGATE CHILD EXPLOITATION IN THE ONLINE ENVIRONMENT, International Journal of Education and Social Science Research (IJESSR) 7 (2): 273-278 Article No. 928, Sub Id 1447

CYBER HYGIENE: ENHANCING CYBER HYGIENE PRACTICES TO MITIGATE CHILD EXPLOITATION IN THE ONLINE ENVIRONMENT

Ifeoluwa Elegbe

Affiliation: Georgia Southern University

DOI: https://doi.org/10.37500/IJESSR.2024.7219

ABSTRACT

The study examines how cyber hygiene reduces online child exploitation. Child exploitation, a term that incorporates a range of abusive and exploitative behaviors, has emerged as a significant and urgent issue in the era of digital technology (UNICEF, 2021). It analyzes current practices, their effects on child safety, and improvement ideas using a literature study. This study advises improving cyber hygiene to reduce online child exploitation. Using a comprehensive literature analysis and systematic review, the study will identify child exploitation vulnerabilities in current cyber hygiene practices and create specific suggestions for individuals, parents, educators, and organizations. Stakeholder feedback will inform incremental changes as the proposed enhancements are pilot tested and validated in real-world circumstances. Policy implications and advocacy for legislative initiatives, industry standards, and stakeholder collaboration to improve cyber hygiene will also be examined. This study seeks to improve children's well-being in the digital age by providing evidence-based online safety strategies. The findings show that user education, technology solutions, and collaboration are needed to safeguard children from online exploitation. The study finishes with recommendations for governments, educators, and technology corporations to improve cyber hygiene and protect children online.

KEYWORDS: Cyber hygiene, child exploitation, victimization, online environment, digital safety, internet safety

INTRODUCTION

Digital technologies and the internet have revolutionized our lives, work, and interactions, but they also pose new challenges, especially in child safety (Livingstone & Haddon, 2009. The online environment has become a breeding ground for child exploitation, including cyberbullying, sexual abuse, and the distribution of harmful content (Kloess et al., 2014). The U.S. Department of Homeland Security's 2021 "National Strategy to Combat Human Trafficking" study speaks regarding digital child exploitation. Child trafficking has escalated due to online activity and social isolation during the COVID-19 pandemic (U.S. Department of Homeland Security, 2021). The issue of child exploitation in the digital realm is an enormous concern, as predators take advantage of the ability to remain anonymous and easily approach young individuals for the purpose of grooming, engaging in sexual abuse, and distributing child sexual abuse material (CSAM) (Whittle et al., 2013). Victims of this type

of exploitation might experience significant physical and psychological repercussions. According to Cybersecurity and Infrastructure Security Agency Cyber hygiene is crucial for children's internet safety, preventing child exploitation and ensuring a secure digital environment for both individuals and businesses (Cybersecurity and Infrastructure Security Agency, 2021). Cyber hygiene practices, including weak passwords, outdated software, and lack of parental supervision, are often exploited by perpetrators to target and victimize children in various online spaces, including social media, messaging apps, and chat rooms.

LITERATURE REVIEW

Online child exploitation

Child exploitation, including sexual abuse, pornography, and online grooming, has become prevalent worldwide (Kloess et al., 2014). Internet anonymity and accessibility allow predators to target and exploit youngsters, frequently with tragic results (Whittle et al., 2013). Digital devices, social media, and online communication tools allow offenders to groom and exploit children in ways that are hard to identify and avoid.

This study considered online child exploitation using social learning and routine activity theories. Albert Bandura's social learning theory states that people learn by seeing, imitating, and reinforcing (Bandura, 1977). Child exploitation perpetrators may learn and imitate exploitative habits from comparable acts. Cohen and Felson's routine activity theory says that motivated offenders, suitable targets, and absence of guardian’s influence crime (Cohen & Felson, 1979). These beliefs apply to online exploitation by vulnerable youngsters, motivated offenders, and poor cyber hygiene.

Cyber hygiene relates to the collection of procedures and behaviors employed by individuals and organizations to protect the security and integrity of their digital systems and data. These practices encompass routine software upgrades, robust password management, and the use of antivirus and firewall security (Whittle et al., 2013). Cyber hygiene involves robust security measures like strong password policies, regular software updates, and secure communication channels (Coventry & Branley, 2018). Nevertheless, their ability to reduce child exploitation in the internet realm is restricted. Conventional cyber hygiene techniques primarily address common cybersecurity risks, overlooking the specific difficulties and susceptibilities related to child exploitation.

Cyber hygiene techniques sometimes neglect the special issues of child abuse, instead focusing on broad cybersecurity concerns such as data breaches and malware. These frameworks fail to account for children's special needs and vulnerabilities (Whittle et al., 2013). The rapid expansion of digital technology, combined with the rising complexity of criminals, necessitates continuous adaptation and enhancement of cyber hygiene procedures. Traditional procedures struggle to keep up with the dynamic online world and child exploiters' ever-changing strategies.

International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 7, Issue.2, March-April 2024, p no. 273-278

Existing Efforts to Address the Issue:

The increasing issue of child exploitation in the online realm has led to the efforts of several groups and projects to raise awareness and adopt technological remedies (Kloess et al., 2014). Nevertheless, their endeavors are frequently constrained by the intricate nature of the problem. An all-encompassing and well-coordinated strategy is required to improve cyber hygiene standards and safeguard children from online exploitation (Kloess et al., 2014). Although there has been improvement, the intricate nature of the problem requires a more extensive and synchronized effort to tackle this increasing danger.

Challenges in Addressing Child Exploitation in the Online Environment

Due to the anonymity and worldwide nature of the internet, rapid technical change, and new digital platforms, addressing child abuse online is difficult (Coventry & Branley, 2018). Online predators' strategies confront parents, schools, and law enforcement. Child Sexual Abuse Material (CSAM), a lucrative and ubiquitous kind of exploitation, perpetuates a cycle of abuse, requiring law enforcement, technological firms, and international organizations to work together (Kloess et al., 2019).

METHODOLOGY

This study uses a literature review to examine how cyber hygiene measures reduce online child exploitation. To understand the issue and find ways to improve cyber hygiene, the study evaluates peer-reviewed journal articles, government reports, and industry recommendations. Key areas of the literature review were:

i. Online child exploitation frequency and impact.
ii. How cyber hygiene reduces child exploitation risks.
iii. Cyber hygiene improvement methods and best practices.
iv. Obstacles to proper cyber hygiene.

The literature review was synthesized to provide a comprehensive understanding of the topic, identify potential solutions, and offer recommendations for policymakers, educators, and technology companies.

RESULT AND DICUSSION

To mitigate the risks of child exploitation in the online environment, a comprehensive conceptual framework for enhancing cyber hygiene practices is proposed. The literature study revealed that cyber hygiene practices reduce the chances of child exploitation online. This framework encompasses three key elements: user education, technological safeguards, and policy and regulatory measures. Cyberbullying, sexual assault, and dangerous content distribution thrive online. Digital technology's anonymity and accessibility make child abuse easier. Child exploitation can cause psychological trauma, social isolation, and developmental difficulties (Finkelhor et al., 2015). Cyber hygiene practices, such as strong passwords, regular software updates, secure browsing habits, and parental controls, are essential in mitigating the risks of child exploitation in the online environment. These practices create a secure and healthy digital environment, reducing the likelihood of children being

exposed to harmful content or predatory behavior (Cybersecurity and Infrastructure Security Agency, 2021).Improved cyber hygiene is essential to combat online child exploitation. Customized education programs can teach children, parents, and educators about online exploitation and cyber hygiene. These programs should teach safe internet use, suspicious activity reporting, and digital security.

Enhancing cyber hygiene requires educating users, especially children and their caregivers, provide online safety advice, identify, and report suspicious activity, and apply personal data protection best practices (Livingstone & Bulger, 2014). Users may protect themselves and their children from exploitation by learning how to keep the internet safe.
Technological measures improve cyber hygiene. Strong encryption, access controls, and content filtering are needed (Rashid et al., 2013). Development and use of powerful analytical tools and algorithms can also detect and mitigate online child exploitation. Technological measures are crucial for improving cyber hygiene practices. This encompasses the execution of resilient security protocols, such as powerful encryption, stringent access controls, and comprehensive content filtering (Rashid et al., 2013). Moreover, the creation and implementation of sophisticated analytical tools and algorithms can aid in the identification and reduction of possible instances of child exploitation in the digital realm.

A comprehensive framework for combating online child exploitation requires effective policy and regulatory measures. Clear and comprehensive laws and regulations that handle digital concerns are needed (Livingstone & Bulger, 2014). Enforcement of these policies and international cooperation can also improve internet security and accountability.

Advanced technologies like content filtering, picture recognition, and data analytics can detect and report child exploitation interactions (Cybersecurity and Infrastructure Security Agency, 2022) To adapt to perpetrator techniques, these solutions should be updated constantly. Technology companies, law enforcement, and child protection organizations must work together to create and implement these solutions (Cybersecurity and Infrastructure Security Agency, 2022 (Kloess et al., 2014) Continuous improvement requires assessing and updating cyber hygiene practices to handle new threats and vulnerabilities. (Kloess et al., 2014). This helps organizations and people protect children from internet exploitation by staying ahead of developing criminals.

Enhancing Cyber Hygiene Practices: Strategies and Recommendations:

Advanced technologies like content filtering, picture recognition, and data analytics can detect and report child exploitation interactions (Cybersecurity and Infrastructure Security Agency, 2022) To adapt to perpetrator techniques, these solutions should be updated constantly. Technology companies, law enforcement, and child protection organizations must work together to create and implement these solutions (Cybersecurity and Infrastructure Security Agency, 2022). Law enforcement, technology corporations, and child protection organizations can collaborate to share information, develop best practices, and combat online child exploitation (Kloess et al., 2014) Continuous improvement requires assessing and updating cyber hygiene practices to handle new threats and vulnerabilities. (Kloess et

al., 2014). This helps organizations and people protect children from internet exploitation by staying ahead of developing criminals.

User education, technology advances, legal and regulatory frameworks, collaborative initiatives, and ongoing monitoring and assessment are key to fighting online child exploitation. It offers extensive teaching programs and awareness campaigns for children, parents, and caregivers on internet safety, suspicious activity detection, and personal data security best practices. Advanced technologies including content filtering, real-time monitoring, anomaly detection algorithms, and secure communication platforms are also recommended. Digital challenges require clear norms and regulations, including data protection and international collaboration in investigating and prosecuting child exploitation instances. To share information and build holistic solutions, parties like government agencies, law enforcement, civil society organizations, and the commercial sector must collaborate.

CONCLUSION

The issue of online child exploitation is a multifaceted problem that demands a comprehensive response, exacerbated by rapid technological advancements and increased internet reliance, and the COVID-19 pandemic's increased demand for child sexual and reproductive health services (CSAM) (Cybersecurity and Infrastructure Security Agency, 2022). This study report promotes cyber hygiene to prevent child victimization online. To execute a comprehensive cyber hygiene strategy, governments, educators, and technology corporations must collaborate.

The process incorporates stakeholder engagement, user education, and robust technical solutions. Stronger cyber hygiene habits can help children, parents, and caregivers navigate the digital world safely, protecting the future generation.

Child exploitation is a global issue requiring varied solutions. Education, technology, and legislation may improve cyber hygiene and promote a safe, accountable online environment. Collaboration and ongoing development can reduce hazards and make the digital future safer.

REFERENCES

Bandura, A. (1977). Social learning theory. Prentice-Hall.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

Cybersecurity and Infrastructure Security Agency. (2021). Cyber hygiene services. Retrieved from https://www.cisa.gov/cyber-hygiene-services

Cybersecurity and Infrastructure Security Agency. (2022). Cyber hygiene. https://www.cisa.gov/cyber-hygiene

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. Maturitas, 113, 48https://doi.org/10.1016/j.maturitas.2018.04.008

Furnell, S. M., & Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. Computer Fraud & Security, 2009(11), 7-11.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. Trauma, Violence, & Abuse, 15(2), 126-139.

Livingstone, S., & Haddon, L. (2009). EU Kids Online: Final report. EU Kids Online.

Livingstone, S., & Bulger, M. E. (2014). A global research agenda for children's rights in the digital age. Journal of Children and Media, 8(4), 317-335. https://doi.org/10.1080/17482798.2014.961496

U.S. Department of Homeland Security. (2021). National strategy to combat human trafficking. https://www.dhs.gov/sites/default/files/2021-12/21_1130_plcy_national-strategy-combat human-trafficking.pdf

U.S. Department of Justice. (2020). Child exploitation and obscenity section. https://www.justice.gov/criminal-ceos

UNICEF. (2021). Online child sexual exploitation and abuse: A global snapshot. https://www.unicef.org/media/105666/file/OCSEA-Global-Snapshot.pdf

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2013). Scoping the cyber security body of knowledge. IEEE Security & Privacy, 11(6), 67-69.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. Aggression and Violent Behavior, 18(1), 62-70.